代数幾何ゼミ

石井大海

早稲田大学基幹理工学部
数学科四年

2013 年 04 月 08 日

Buchberger アルゴリズムの改良

- 実際に Buchberger アルゴリズムを実装してみた.
  - Singular などに較べて 1000 倍くらい遅い！

  $\Rightarrow$ 何とか 100 倍くらいにしたいのでこの節から始めます.
- 数学ソフトウェア：正確性だけでなく速度も大事.
  - 大抵の計算代数ソフトウェアに含まれている改良法について.
  - Buchberger アルゴリズムの計算量についても議論
  - まだ枯れていない分野，らしい

Buchberger アルゴリズムの核は何か？

Th. (Buchberger 判定法)

$G : I$ の基底 とするとき，次が成立.

$$\forall g_i, g_j \in G \left[\overline{S(g_i, g_j)}^{G} = 0 \right] \Leftrightarrow G \text{ は } I \text{ の } \textit{Gröbner} \text{ 基底}$$

- 多項式の割り算は計算量を喰う.
  - $\Rightarrow$ 割り算の回数を減らせないか？
- 無視出来る S-多項式は何か？を考えるために Buchberger 判定法の証明を復習してみる

Buchberger 判定法の証明 I

次の補題を使う（証明は略）.

Lemma.

$f = \sum_{i=1}^{s} c_i f_i \quad (c_i \in k, f_i \in k[\mathbf{X}], \deg f_i = \delta \in \mathbb{Z}^n_{\geq 0})$ とする．このとき，$\deg f < \delta$ ならば，f は $1 \leq j, k \leq s$ について $S(f_j, f_k)$ の k-線型結合で書け，しかも $S(f_j, f_k) < \delta$ となる.

(⇐) の証明 G を I の Gröbner 基底とすると，$g_i, g_j \in \langle G \rangle = I$ なので，$S(g_i, g_j) \in I$. よって系 6.2 より $\overline{S(g_i, g_j)}^{G} = 0$ となる. ∎

Buchberger 判定法の証明 II

(⇒) の証明 G が Gröbner 基底であることを示すには，$LT(I) = \langle LT(g_1), \ldots, LT(g_t) \rangle$ を示せばよい．そこで，$f \in I \setminus \{0\}$ として，

$$LT(f) \in \langle LT(g_1), \ldots, LT(g_t) \rangle$$

を示そう．$f \in I = \langle G \rangle$ より，$h_i \in k[\mathbf{X}]$ によって

$$f = \sum_{i=1}^{t} h_i g_i \tag{1}$$

と表せる．この時明らかに，

$$\deg f \leq \max_{1 \leq i \leq t} \deg(h_i g_i)$$

が成立している．補題 6.5 より，もし等号が不成立ならどこかで先頭項が打消し合うものが存在して，

Buchberger 判定法の証明 III

それを g_i, g_j の S-多項式を用いて書き直すことが出来，しかも $S(g_i, g_j) < \max_{1 \leq i \leq t} \deg(h_i g_i)$ と出来る．よって，$m(i) = \deg(h_i g_i), \delta = \max_{1 \leq i \leq t} m(i)$ とすれば，$\deg f \leq \delta$ とできる．

さて，(1) のように表わす方法は一意ではないので，そうした線型和を全て考えて，その中で δ が最小となるようなものを考えよう（単項式順序の整列性より常に存在する）．この時，特に $\deg f = \delta$ となれば，ある i により $LM(f) = LM(g_i)$ となり $LM(f) \in \langle LT g_1, \ldots, LT g_t \rangle$ となり証明が完了する．

今，$\deg f < \delta$ とすると，上の議論から打消し合う先頭項どうしが存在する．$h_{j_1} g_{j_1} + \cdots + h_{j_k} g_{j_k}$ と置くと，これは k-係数の S-多項式の線型和で表せる：

$$h_{j_1} g_{j_1} + \cdots + h_{j_k} g_{j_k} = \sum_{i=1}^{s-1} c_i S(g_{j_i}, g_{j_{i+1}})$$

Buchberger 判定法の証明 IV

また，しかも $\deg S(g_{j_i}, g_{j_{i+1}}) < \delta$ となるように取れる．今，$\overline{S(g_i, g_j)}^{G} = 0$ であったから，除算アルゴリズムの性質より

$$\begin{cases} S(g_{j_k}, g_{j_\ell}) = \sum_{i=1}^{t} c_{ik\ell} g_i \\ \deg(c_{ik\ell} g_i) \leq \deg S(g_{j_k}, g_{j_\ell}) \end{cases} \tag{2}$$

Buchberger 判定法の証明 V

となるような $c_{ik\ell} \in k[\mathbf{X}]$ が取れる．よって，

$$\begin{aligned}
\sum_{i=1}^{s} h_i g_i &= \sum_{m(i)=\delta} h_i g_i + \sum_{m(i)<\delta} h_i g_i \\
&= \sum_{i=1}^{s-1} c_i S(g_{j_i}, g_{j_{i+1}}) + S \\
&= \sum_{i=1}^{s-1} c_i \sum_{\ell=1}^{t} c_{\ell i i+1} g_\ell + S \\
&= \sum_{i=1}^{s-1} \sum_{\ell=1}^{t} c_i c_{\ell i i+1} g_\ell + S \\
&= \sum_{i=1}^{t} \bar{h}_i g_i + S
\end{aligned}$$

Buchberger 判定法の証明 VI

このとき，定義より明らかに $\deg S < \delta$ であり，上の条件から $\deg c_i c_{\ell i(i+1)} g_\ell \leq \deg S(g_i, g_{i+1}) < \delta$ となる．よって，新しく得られた $\bar{h}_i$ と S によって f を書き直してやれば，δ よりも真に小さな多重次数を持つ線型和が取れる．しかし，これは δ の最小性に矛盾．

よって以上から，$\deg f = \delta = \max_{1 \leq i \leq t} \deg h_i g_i$ となり，特に $LT(f) = h_i LT(g_i)$ となるような i が取れるので，G は Gröbner 基底であることがわかった．

ゼロ簡約 I

この証明を良く見ると，本質的な役割を果しているのは条件 (2) である事がわかる．そこで，この条件を取り出して新しい条件を定義しよう．

Def. 1 (ゼロ簡約)

単項式順序を一つ固定し，$G = \{ g_1, \ldots, g_t \} \subseteq k[\mathbf{X}]$ とする．

$$f \in k[\mathbf{X}] \text{ が } G \text{ を法としてゼロに簡約される}$$

$$\overset{\text{def}}{\Longleftrightarrow} \begin{cases} f = a_1 g_1 + \cdots + a_t g_t \\ a_i g_i = 0 \text{ または } \deg(f) \geq \deg(a_i g_i) \end{cases}$$

このとき，$f \underset{G}{\longrightarrow} 0$ と書く．

ゼロ簡約 II

除算アルゴリズムから，明らかに次が成立（逆は一般に不成立）.

Lemma 2

$$\overline{f}^{G} = 0 \Rightarrow f \underset{G}{\longrightarrow} 0$$

Example. (不成立の例)

$G = (XY - 1, X^2 + Y), f = (X^2 + Y)(X - 1) + (YX - 1) \underset{G}{\longrightarrow} 0.$

しかし，$\overline{f}^{G} = 2Y - 1.$ ∎

ゼロ簡約を用いた判定法 I

これを用いて，Buchberger 判定法を書き直したのが次.

Th. 3

改良 *Buchberger* 判定法 $G : I$ の基底 とするとき，次が成立.

$$\forall g_i, g_j \in G \left[S(g_i, g_j) \underset{G}{\longrightarrow} 0 \right] \Leftrightarrow G \text{ は } I \text{ の } \textit{Gröbner} \text{ 基底}$$

- 証明は上のをなぞるだけ.
- 古い Buchberger 判定法 はこれと補題 2 の系.

  $\Rightarrow$ では，具体的にゼロに簡約される条件は何か？

ゼロ簡約を用いた判定法 II

Prop. 4

$G \Subset k[\mathbf{X}]$: 有限集合 とする． $f, g \in G$ について次が成立.

$$LCM(LM(f), LM(g)) = LM(f)LM(g) \Rightarrow S(f, g) \underset{G}{\longrightarrow} 0$$

即ち，二つの多項式の先頭単項式が互いに素ならば，その S-多項式はゼロに簡約される.

ゼロ簡約を用いた判定法 III

Proof.

f, g の係数は共に 1 であるとして一般性を失わない．そこで $f = LM(f) + p, g = LM(g) + q$ と置くと，$LCM(LM(f), LM(g)) = LM(f)LM(g)$ より，

$$\begin{aligned} S(f,g) &= LM(g)f - LM(f)g \\ &= (g-q)f - (f-p)g \\ &= fg - qf - fg + pg = pg - qf \end{aligned}$$

となる．ここで，$\max\{\deg(pg), \deg(qf)\} = \deg S(f,g)$ となる．もし S-多項式の次数の方が小さいとすると，pg, qf の先頭項同士は打消し合うことになる．すると，$LM(p)LM(g) = LM(q)LM(f)$ となるが，今 $LM(g), LM(f)$ は互いに素なので，$LM(g) \mid LM(q)$ となる．しかし，これは $LM(g)$ が g の先頭項であることに矛盾．よって，$S(f,g)$ は $f, g \in G$ にの線型和で表せ $S(f,g) \underset{G}{\longrightarrow} 0$. ∎

互いに素チェックは上手くいくのか？

これで果してどれくらい計算量が節約されるのか？

Example. (上手く行く例)

$G = (yz + y, x^3 + y, z^4)$ とし，単項式順序として grlex を採用する．この時，x^3, z^4 は互いに素なので，上の命題より $S(x^3 + y, z^4) \xrightarrow[G]{} 0$ となる．しかし，$S(x^3 + y, z^4) = yz^4$ であり，

$$\overline{S(x^3 + y, z^4)}^{G} = y \neq 0$$

となることがわかる．このようにして S-多項式とその余りを計算することなく，不必要な基底を取り去ることができる．

- 先頭項が互いに素でない時だけ S-多項式 を計算すればよい
- これだけでもかなり高速化される（ベンチを後程）

そもそも S-多項式とはなんなのか？ I

- 更なる高速化のために，そもそも S-多項式の役割とは何なのかを考える
- S-多項式とは先頭項を打消し合ったもの.

$\Rightarrow$ 「打消し合い」をより一般的に考察すべし！

Def. 5 (先頭項の syzygy)

$(h_1, \ldots, h_s) \in k[\mathbf{X}]^s$が $F = (f_1, \ldots, f_s)$ の先頭項上の syzygy

$$\overset{\text{def}}{\Longleftrightarrow} \sum_{i=1}^{s} h_i LT(f_i) = 0$$

以下，F の先頭項上の syzygy の全体を $S(F)$ と書く.

そもそも S-多項式とはなんなのか？ II

Example.

$F = (x, x^2 + xz, y + z)$ に対し，$(-x + y, 1, -x) \in k[\mathbf{X}]^3$ は F の syzygy であり，$S(F)$ に属する：

$$\begin{aligned}
&(-x + y) \cdot x + 1 \cdot (x^2 + xz) + (-x) \cdot (y + z) \\
&= -x^2 + xy + x^2 + xz - xy - xz \\
&= 0
\end{aligned}$$

S-多項式と syzygy

syzygy を綺麗に書くために次のような記法を考える．
$\mathbf{e}_i = (0, \ldots, 0, 1, 0, \ldots, 0)$（第 i 成分のみ 1）というような「ベクトル」を考えると，$S(F)$ の元は $S = \sum_{i=1}^{s} h_i \mathbf{e}_i$ と書ける．これを使って，まず S-多項式が syzygy を定めることを云う．
$f_i, f_j \in F, \mathbf{X}^\gamma = LCM(LM(f_i), LM(f_j))$ とおく．このとき，

$$S_{ij} = \frac{\mathbf{X}^\gamma}{LT(f_i)}\mathbf{e}_i - \frac{\mathbf{X}^\gamma}{LT(f_j)}\mathbf{e}_j \tag{3}$$

を考えると，これは F の先頭項上の syzygy になっている：

$$S_{ij} \cdot LT(F) = \frac{\mathbf{X}^\gamma}{LT(f_i)}LT(f)_i - \frac{\mathbf{X}^\gamma}{LT(f_j)}LT(f_j) = 0$$

実際，S-多項式の S は syzygy の S.

syzygy の「基底」と斉次 syzygy I

- $S(F)$ は定義から明らかに加法と $k[\mathbf{X}]$ による「スカラー倍」によって閉じている（つまり $k[\mathbf{X}]$-加群になる）。
- 更に、$S(F)$ は有限基底を持つ
  - syzygy はある有限個の syzygy の $k[\mathbf{X}]$-線型和で書ける！
  - 証明の為、まず「斉次 syzygy」の概念を定義する。

Def. 6 (斉次 syzygy)

$S \in S(F)$ が次数$\alpha \in \mathbb{Z}^n_{\geq 0}$の斉次 syzygy

$$\overset{\text{def}}{\Longleftrightarrow} \begin{cases} S = (c_1 \mathbf{X}^{\alpha(1)}, \ldots, c_s \mathbf{X}^{\alpha(s)}) & (c_i \in k) \\ c_i \neq 0 \Rightarrow \alpha(i) + \deg(f_i) = \alpha & (1 \leq i \leq s) \end{cases}$$

（単項式から成り F との各成分の積の最高次数が一定な syzygy）

例えば、(3) における S_{ij} は次数 γ の斉次 syzygy。

syzygy の「基底」と斉次 syzygy II

実は、斉次 syzygy が $S(F)$ の基底になっている。

Lemma 7

$S(F)$ の任意の元は、$S(F)$ の斉次 *syzygy* の和で一意に表わされる。

存在性.

$S = (h_1, \ldots, h_s) \in S(F)$ として、指数 $\alpha \in \mathbb{Z}^n_{\geq 0}$ を一つ固定しよう。もし $\deg(h_{i\alpha} f_i) = \alpha$ となるような h_i の項があればそれを $h_{i\alpha}$ と置く。このとき、$\sum_{i=1}^{s} h_{i\alpha} LT(f_i) = 0$ となる。なぜなら、S は syzygy なので $\sum_{i=1}^{s} h_i LT(f_i) = 0$ であり、$\sum_{i=1}^{s} h_{i\alpha} LT(f_i)$ はこの和の次数 α の成分となるからである。そこで、
$S_\alpha = \{ h_{1\alpha}, \ldots, h_{s\alpha} \}$ と置けば、これは斉次 syzygy であり、
$S = \sum_\alpha S_\alpha$ となる。 ∎

syzygy の「基底」と斉次 syzygy III

一意性（演習 5）.

$S = \sum_\alpha S_\alpha = \sum_\alpha S'_\alpha$ （各 S_α, S'_α は次数 α の斉次 syzygy）と表わせたとする。S_α, S'_α の第 i 成分をそれぞれ $h_{i\alpha}, h'_{i\alpha}$ とすれば、

$$h'_{i\alpha} = 0 \vee \deg(h'_{i\alpha}) = \alpha - \deg(f_i)$$

となる（h についても同様）。$h'_{i\alpha} = 0$ とすると、S の第 i 成分の α 次の項はゼロとなるので、 $h_{i\alpha} = 0$ とならなくてはならない。$h'_{i\alpha} \neq 0$ とするとさっきの項はゼロにならず、従って $\deg(h'_{i\alpha}) = \alpha - \deg(f_i) = \deg(h_{i\alpha})$ となり、両者は一致する。よって各 S_α, S'_α の各成分が一致するので、S は斉次 syzygy により一意に表すことが出来る。 ∎

syzygy の「基底」と斉次 syzygy IV

更に、$S(F)$ の斉次基底として (3) の S_{ij} を取ることが出来る、というのが次の命題である。

Prop. 8

$F = (f_1, \ldots, f_s)$ の先頭項任意の *syzygy* $S \in S(F)$ は、(3) の S_{ij} を用いて、

$$S = \sum_{i<j} u_{ij} S_{ij} \quad (u_{ij} \in k[\mathbf{X}])$$

の形に表せる。

syzygy の「基底」と斉次 syzygy V

証明の概略.

補題 7 より、S は零でない斉次 syzygy であるとしてよい。よって、S は少なくとも二つの非零成分 $c_i\mathbf{X}^{\alpha(i)}, c_j\mathbf{X}^{\alpha(j)}$ $(i<j)$ を持ち、$\alpha(i)+\deg(f_i)=\alpha=\alpha(j)+\deg(f_j)$ 。ここで $\mathbf{X}^\alpha$ を f_i, f_j の先頭項の LCM とおけば、$\mathbf{X}^\gamma \mid \mathbf{X}^\alpha$ となる。今、

$$S - c_i LC(f_i) X^{\alpha-\gamma} S_{ij} \qquad (*)$$

の i 成分について考えると、S_{ij} の定義から、

$$\begin{aligned} & c_i\mathbf{X}^{\alpha(i)} - c_i LC(f_i) X^{\alpha-\gamma}\mathbf{X}^\gamma / LT(f_i) \\ &= c_i\mathbf{X}^{\alpha(i)} - c_i LC(f_i)\mathbf{X}^{\alpha-\gamma}\mathbf{X}^\gamma / (X^{\deg(f_i)} LC(f_i)) \\ &= c_i\mathbf{X}^{\alpha(i)} - c_i\mathbf{X}^{\alpha-\gamma+\gamma-\deg(f_i)} = c_i\mathbf{X}^{\alpha(i)} - c_i\mathbf{X}^{\alpha(i)} = 0 \end{aligned}$$

となる。これにより非零成分が一つ減り後は繰り返せばよい。 ∎

syzygy の基底と Gröbner 基底

このような「syzygy の基底」を考えると何が嬉しいのか？実は次の定理が成立する。

Th. 9

イデアル I の基底 $G = (g_1, \ldots, g_t)$ について、次の二つは同値。

- G が I の *Gröbner* 基底
- *syzygy* $S(G)$ の任意の斉次基底 S に対し、

$$S \cdot G = \sum_{i=1}^{t} h_i g_i \underset{G}{\longrightarrow} 0$$

今までの素朴な Buchberger アルゴリズムは、$S(G)$ の基底として特に S_{ij} を使ったものだった。もしこの基底に「余分な」元があれば、そいつを予め取り除いてやることで、より効率がよくなる筈。

定理9 の証明 I

Buchberger 判定法の証明を繰り返す。まず $(\Leftarrow)$ を考える。特に、

$$f = \sum_{i=1}^{t} h_i g_i \quad m(i) = \deg(h_i g_i) \quad \delta = \max_{1 \leq i \leq t} m(i)$$

とし、$LT(f) \in \langle LT(g_1), \ldots LT(g_t) \rangle$ を示す。今までの証明と同様、δ が最小となるような h_i, g_i をとり、$\deg(f) < \delta$ を仮定して矛盾を導けばよい。
$\deg(f) < \delta$ より $\sum_{m(i)=\delta} LT(h_i)LT(g_i) = 0$ となることに注意すれば、

$$S = \sum_{m(i)=\delta} LT(h_i)\mathbf{e}_i$$

は G の syzygy を定める。また、i の取り方より、これは次数 δ の斉次 syzygy である。

定理 9 の証明 II

今、斉次基底 $S_1, \ldots, S_m$ により、

$$S = u_1 S_1 + \ldots, u_m S_m$$

と書け、特に仮定より $S_j \cdot G \underset{G}{\longrightarrow} 0 \quad (1 \leq j \leq m)$ が成立する。ここで S は斉次 syzygy であるので、各 j について $u_j S_j = 0$ であるか $u_j S_j$ が次数 δ の斉次 syzygy となっているとしてよい。
S_j が次数 γ_j の斉次 syzygy とすれば、 $u_j \neq 0$ の時
$u_j = c_j \mathbf{X}^{\delta - \gamma_j} \quad (c_j \in k)$ と書ける。よって、

$$S = \sum_{u_j \neq 0} c_j \mathbf{X}^{\delta - \gamma_j} S_j$$

となる。両辺を G について内積を取れば、

$$\sum_{m(i)=\delta} LT(h_i) g_i = S \cdot G = \sum_i c_i \mathbf{X}^{\delta - \gamma_i} S_i \cdot G.$$

定理 9 の証明 III

ここで仮定より $S_j \cdot G \underset{G}{\longrightarrow} 0$ より、

$$\begin{cases} S_j \cdot G = \sum_{i=1}^{t} a_{ij} g_i \\ \deg(a_{ij} g_i) \leq \deg(S_j \cdot G) \end{cases}$$

が成立。あとは、

$$\deg(\mathbf{X}^{\delta - \gamma_i} S_i \cdot G) < \delta$$

が示せれば、前の議論と同様にして証明が完了する。これは

$$\delta - \gamma_i + \deg(S_i \cdot G) < \delta$$
$$\therefore \deg(S_i \cdot G) < \gamma_i$$

と同値だから、こちらを示せばよい（演習 6）。S_i は次数 γ_i の斉次 syzygy だったから、

$$S_i \cdot LT(G) = 0$$

定理 9 の証明 IV

となる。これにより、$S_i \cdot LT(G)$ の γ_i 次の項は全て消えることがわかる。よって $\deg(S_i \cdot G) < \gamma_i$ となる。よって、最小である筈の次数 δ を下回るような分解が取れて矛盾する。
$(\Rightarrow)$ について。G を Gröbner 基底、S を斉次 syzygy とすると、$S \cdot G = \sum h_i g_i \in I$ である。よって Gröbner 基底の性質から $\overline{S \cdot G}^{G} = 0$ となり、補題 2 より $S \cdot G \underset{G}{\longrightarrow} 0$ となる ∎

無駄な基底の判定 I

- S_{ij} ではなく syzygy の斉次基底を考えればよいことが判った。
- 必要な基底が S_{ij} 全体よりも少なければ無駄が省ける！
- 本当にそんな場合があるの？
  - 例：$F = (x^2y^2 + z, xy^2 - y, x^2y + yz)$ の syzygy の S-多項式による基底は、

    $$S_{12} = (1, -x, 0) \quad S_{13} = (1, 0, -y) \quad S_{23} = (0, x, -y)$$

    だが、 $S_{13} - S_{12} = (0, x, -y) = S_{23}$ となるので、実際には S_{23} は不要！
- どういう場合にこういったことが起こりうるのか？

無駄な基底の判定 II

Prop. 10

$G = (g_1, \ldots, g_t)$　$\mathcal{S} \subseteq \{ S_{ij} \mid 1 \leq i < j \leq t \}$: $S(G)$ の基底とする。このとき次が成立。

$g_i, g_j, g_k \in G$ があって $LT(g_k) \mid LCM(LT(g_i), LT(g_j))$ かつ $S_{ik}, S_{jk} \in \mathcal{S}$ となるとき、$\mathcal{S} \setminus \{S_{ij}\}$ も $S(G)$ の基底となる。

Proof.

簡単の為 $i < j < k$ とする。$\mathbf{X}^{\gamma_{ij}} = LCM(LM(g_i), LM(g_j))$ とおき、jk, ik についても同様に定める。このとき、仮定から $\mathbf{X}^{\gamma_{ik}}, \mathbf{X}^{\gamma_{jk}}$ は共に $\mathbf{X}^{\gamma_{ij}}$ を割り切る。すると、

$$S_{ij} = \frac{\mathbf{X}^{\gamma_{ij}}}{\mathbf{X}^{\gamma_{ik}}} S_{ik} - \frac{\mathbf{X}^{\gamma_{ij}}}{\mathbf{X}^{\gamma_{jk}}} S_{jk}$$

となり、よって S_{ij} を取り去っても基底となる。 ∎

改良型 Buchberger アルゴリズム

互いに素の判定と syzygy の基底を用いて高速化したものが次。

Th. 11 (改良型 Buchberger アルゴリズム)

次の手順により *Gröbner* 基底が求められる。

入力 $F = (f_1, \ldots, f_s)$

初期化 $B := \{ S_{ij} \mid 1 \leq i < j \leq s \}$ $G := F$ $t := s$

手順 $B = \emptyset$ となるまで以下を繰り返す：

1. $(i, j) \in B$ を任意に選ぶ。
2. $LCM(LT(f_i), LT(f_j)) \neq LT(f_i)LT(f_j)$ かつ判定 (f_i, f_j, B) が偽なら次を実行
   - (i) $S := \overline{S(f_i, f_j)}^{G}$
   - (ii) $S \neq \emptyset$ ならば $t += 1$ $f_t = S$ $G := G \cup \{f_t\}$ $B := \{ (i, t) \mid 1 \leq i \leq t-1 \}$
3. $B := B \setminus \{(i, j)\}$

出力 G

但し、判定は $(i, k), (j, k) \notin B$ かつ $LT(f_k) \mid LCM(LT(f_i), LT(f_j))$ となるような $k \neq i, j$ があるとき真とする。

アルゴリズムの解説

- 基本的なアイデア：B に「検討すべき基底の候補」を記録しておく。
- 先頭項が互いに素なら追加の必要はなく、余分な基底は命題 10 を使って取り除ける
  - どちらも使えなかったら、S_{ij} を追加する。
- もし一番内側の条件分岐が実行されて G が増えると、$\langle LT(G) \rangle$ は増大する。Noether 性からこの増加は必ず有限回で止まる。
- あとは B の要素がループ毎に減っていくので、アルゴリズムは必ず有限回で停止する。

更なる改良（ヒューリスティクス）

これは勿論、まだまだ最適ではない。幾つか改善法がある。

- 上のアルゴリズムには幾つか自由度がある。
  - (i) で S 多項式を割る際、G の並び順は任意。
    - そこで、使っている単項式順序で昇順に並べておくと、最初の内に沢山割れて割るステップが小さくなるのではないか？
  - (1) ではどんな風に f_i, f_j を選んでもよい

    標準戦略　先頭項の LCM が現在の単項式順序で最小となるように選ぶ（Buchberger）。

    Sugar　上の方法は、次数と両立しない単項式順序（例えば Lex）を利用した時に上手くいかない。そこで、sugar と呼ばれる仮想的な斉次化次数を考える。
- いずれもヒューリスティクスだが、割と速度が改善される。

Sugar Strategy

- 良く知られている（らしい）ヒューリスティクス：生成元を斉次化してから Buchberger を使うと速く終わり易い
- 問題点：得られた基底から余分な文字を消去しても、元のイデアルの Gröbner 基底になっているとは限らない！
  - Gröbner になっていなかったら、その基底に対してもういちど Buchberger したりする。
  - そこで、(i, j) を選ぶ時にだけ仮想的に斉次化して最小の物を選ぶとどうか？
  - それだけだと同率一位が出て来るので、標準戦略 + アルゴリズムで早く出て来た物を選ぶ。
    - 最後の条件は原論文にはちょろっとしか書いていないのだけど、これをするかしないかで二倍くらい時間がかわる……。
- この仮想的な斉次化次数のことを「sugar」と呼ぶ。
- 原論文ではかなりの高速化を達成している。
  - 私の実装では余り速くならなかったので、データ構造を見直し中……。

ベンチ：どれくらい速くなるのか？

詳細は別紙（１・２）を参照。

- 互いに素の判定を入れただけでも大体 5〜10 倍速くなる。
  - 勿論指数二乗オーダーなので「倍」という表現はおかしいが……
- 更に syzygy の基底判定を入れると、最大で元の約 100 倍（！！）速くなる！
- それでもまだ Singular よりは遅いです（とーぜん）。
- 例えば、Singular では cyclic 5：

$$I = \left\langle \begin{matrix} a+b+c+d+e, ab+bc+cd+de+ea, abc+bcd+cde+dea+eab, \\ abcd+bcde+cdea+deab+eabc, abcde-1 \end{matrix} \right\rangle$$

の Lex に関する Gröbner 基底は一瞬で求まるが、私の実装では二、三分経っても終わらない（orz）。

Buchberger アルゴリズムの計算量 I

- 現在知られている最良の実装でも時間と領域を食い潰すような入力が簡単に作れる。
  - アルゴリズムの途中で生成される多項式の次数がとても大きい
  - 生成元の係数が小さな整数でも、Gröbner 基底の係数は複雑な有理数になる場合がある。
- 多項式の次数の上限は、入力の次数 d に対し理論的に 2^{2^d} であると示されていて、実際そうなる例も構成されている。
- これはあっというまに発散するので Grevlex でも歯が立たない。たとえば、$x^{n+1} - yz^{n-1}w, xy^{n-1} - z^n, x^n z - y^n w$ について Grevlex で計算すれば、$x^{n^2+1} - y^{n^2} w$ が必ずその中に含まれる、というような事が知られている。
- 三変数の場合はもっとお手軽な上界が得られるので悲観しなくてよいらしい。

Buchberger アルゴリズムの計算量 II

- 幾何学的に意味のある例の殆んどは、上の上界よりも「平均で」かなりお手頃な計算量で済む、らしい。
- 変数の置き換えや順序の選択で劇的に計算が簡単になる。
  - Grevlex が大抵の場合において一番次数の小さな基底を齎すことがわかっている。(そうでない例：演習問題 13)

$$I = \langle a^4 - bc^2d, ab^2 - c^3, a^3c - b^3d \rangle$$

$$G_{lex}(I) = \left\langle \begin{matrix} ab^2-c^3, & -c^{10}+b^9d, & a^4-bc^2d, \\ a^3c-b^3d, & a^2c^4-b^5d, & ac^7-b^7d \end{matrix} \right\rangle$$

$$G_{grevlex}(I) = \left\langle \begin{matrix} ab^2-c^3, & c^{10}-b^9d, & a^4-bc^2d, \\ a^3c-b^3d, & a^2c^4-b^5d, & ac^7-b^7d \end{matrix} \right\rangle$$

  - 効率的な基底を求めるために、アルゴリズムの途中で単項式順序を変える実装もある。

演習問題：一般の syzygy について

Exercise 2-2

$G = (g_1, \ldots, g_s) \in k[\mathbf{X}]^s$ の *syzygy* $S = (h_1, \ldots, h_s)$ とは、$\sum_{i=1}^{s} h_i g_i = 0$ となるようなものの事。先頭項、という制限を外した。

(a) $G = (x^2 - y, xy - z, y^2 - xz)$ のとき、$(z, -y, x)$ が G の *syzygy* となることを示せ。

(b) 他に *syzygy* を挙げよ。

(c) G 上の *syzygy* は和と $k[\mathbf{X}]$ 倍について閉じることを示せ。

(a) 代入するだけ。

(b) 符号を反転した $(-z, y, -x)$ や、$(y, -x, 1)$ などがそう。

(c) 明らか。

演習問題：判別式イデアルの syzygy I

Exercise 2-3

$M : (m+1) \times m$ 行列　($k[\mathbf{X}]$ 成分) とする、このとき、

$$I := \left\langle \det N \,\middle|\, N : M \text{ の部分行列} \right\rangle$$

により I を定める。このような I を M の行列式イデアルという。

(a) 演習問題 2 の G を生成元とする行列式イデアルを持つような行列 M を見付けよ。

(b) 演習問題 2 を M を使って説明せよ。

(c) 行列式イデアルの生成元の *syzygy* を自動的に生み出す方法を与えよ。

(a) $M = \begin{pmatrix} x & y & z \\ 1 & x & y \end{pmatrix}$ を考えれば、これが求めるもの。

演習問題：判別式イデアルの syzygy II

(b) M の一番上に一行追加した、

$$M' = \begin{pmatrix} x & y & z \\ x & y & z \\ 1 & x & y \end{pmatrix}$$

を考える。この行列式は $\det M' = 0$ となるが、これを一行目について余因子展開すれば、

$$\begin{aligned} \det M' &= (-1)^{1+1} x \cdot \begin{vmatrix} y & z \\ x & y \end{vmatrix} + (-1)^{1+2} y \cdot \begin{vmatrix} x & z \\ 1 & y \end{vmatrix} + (-1)^{1+3} z \cdot \begin{vmatrix} x & y \\ 1 & x \end{vmatrix} \\ &= x \cdot (y^2 - zx) + (-y) \cdot (xy - z) + z \cdot (x^2 - y) \end{aligned}$$

となる。このときの各係数について注目すると、これは G の syzygy となっていることがわかる。(b) で提示した $(y, -x, 1)$ も同様である。このようにして、行列式イデアルの生成元に

演習問題：判別式イデアルの syzygy III

対する syzygy は、行列式をゼロとするような行として得られる。
(c) の性質は、行列式のよく知られた性質（各行は線型）から従う。

(c) 以上から、行列式イデアルの基となる行列に一行足して行列式がゼロとなるようなものが、その生成元の syzygy となり、逆も成立することがわかる。$I \neq 0$ とすれば、G の何処かにはゼロでない行が存在するので、それを取ってくれば syzygy がひとつ得られる。ゼロでない行が複数ある場合、それらの線型和が再び syzygy となっていることも判る。

残りの演習問題については、計算で確認するのと、発表の証明中で証明したものが大半のため省略。